APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/808,911	03/14/2001	Eric Victor Siegel	KAQ-002	4876

959   7590   06/24/2004

LAHIVE & COCKFIELD, LLP.
28 STATE STREET
BOSTON, MA   02109

EXAMINER
MAURO JR, THOMAS J

ART UNIT	PAPER NUMBER
2143	

DATE MAILED: 06/24/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)
Office Action Summary	09/808,911	SIEGEL ET AL.
	Examiner	**Art Unit**
	Thomas J. Mauro Jr.	2143

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>14 March 2001</u>.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-26</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-26</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>14 March 2001</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date <u>1/6/2003</u>.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____ .

DETAILED ACTION

1.   Claims 1-26 are pending and are presented for examination. A formal action on the

merits of claims 1-26 follows.

Specification

2.   The disclosure is objected to because of the following informalities: Page 4 line 34 of the

specification does not provide the meaning/definition of the acronym "PMT" to properly allow

one of skill in the art to understand its meaning.

Appropriate correction is required.

Claim Objections

3.   Claims 4-7 are objected to because of the following informalities: they each depend from

the wrong claim. Claim 4 is dependent upon itself, which is improper. Examiner interprets this

error to be a typo, which for purposes of examination, has been interpreted as "The method of

claim 3." In addition, claims 5-7 have also been interpreted as "The method of claim 3."

Appropriate correction is required.

Claim Rejections - 35 USC § 102

4.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5.   Claims 1-3, 8, 11, 13 and 20-25 are rejected under 35 U.S.C. 102(e) as being anticipated

by Fortenberry et al. (U.S. 6,005,939).

With respect to claim 1, Fortenberry teaches, a method, comprising the steps of:

providing a user profile holding information regarding a user **[Fortenberry -- Col. 1**

lines 51-55 and Col. 5 lines 62-67 – Col. 6 lines 1-7 – Users store certain personal and

demographic information in a database as a profile, i.e. passport];

establishing a first set of permissions for the user profile, wherein said first set of

permissions specifies who may access the user profile **[Fortenberry -- Col. 6 lines 37-46 and**

Col. 8 lines 31-33 – User establishes a first set of permissions with vendors to specify who

can have access to the site by providing them with one or more of a number of keys];

establishing a second set of permissions for a selected sub-division of the user profile,

wherein said second set of permissions specifies who may access the sub-division **[Fortenberry**

-- Col. 6 lines 1-2 and Col. 7 lines 24-33 and lines 51-67 – User establishes a second set of

permissions which provide individual security for various fields stored within the passport.

These dictate who may access the various fields by who the user sends the various keys to,

each containing different access capabilities. Only users who receive keys which allow

access to these permission levels will be able to access these fields]; and

wherein in order for a party to access the selected sub-division, the party must be

specified by the first set of permissions as having access to the user profile and must be specified

by the second set of permissions as having access to the selected sub-division [**Fortenberry --**

Col. 6 lines 15-22 and lines 37-46 and Col. 8 lines 31-32 – In order for a party, i.e. vendor,

to access the information, user must first provide them with a key to access the

information. A second permission, namely, the type of key given to the vendor determines

which information from the individual fields can be accessed by the vendor].

With respect to claim 2, Fortenberry further teaches wherein the sub-division is a field

[**Fortenberry -- Col. 6 lines 1-2 and lines 52-55 and Col. 7 lines 24-33 – Each piece of**

information supplied by a user is a field, i.e. name, address, etc., which contains its own

security policy].

With respect to claim 3, Fortenberry further teaches wherein the first set of permissions

specifies what type of access to the user profile is granted to those who may access the user

profile [**Fortenberry -- Col. 6 lines 37-46 and Col. 8 lines 31-32 – Type of access given to**

vendor is determined by type of key given by user, i.e. first key accesses confidential

information, second key accesses secret information and a third key accesses top secret

information].

With respect to claim 8, Fortenberry further teaches wherein the second set of permissions specifies who may access the user profile **[Fortenberry -- Col. 6 lines 1-2 and Col. 7 lines 24-33 and lines 51-67 – User establishes a second set of permissions which provide individual security for various fields stored within the passport. These dictate who may access the various fields by who the user sends the various keys to, each containing different access capabilities for accessing the user profile fields]**.

With respect to claim 11, Fortenberry further teaches wherein the user specifies at least one of the first set of permissions and the second set of permissions **[Fortenberry -- Col. 7 lines 24-33 and lines 51-60 – User sets priority information for the various fields, i.e. second permissions]**.

With respect to claim 13, Fortenberry further teaches establishing a third set of permissions for an additional field, wherein said third set of permissions specifies who may access the additional field **[Fortenberry -- Col. 6 lines 1-2 and Col. 7 lines 24-33 and lines 51-67 – User establishes a set of permissions for each field within his or her profile which provide individual security for the various specified fields stored within the passport. Only users who receive keys which allow access to these permission levels will be able to access these fields]**.

With respect to claim 20, Fortenberry teaches a method, comprising the steps of:

providing a user profile having various fields, wherein at least one of said fields has

associated permissions **[Fortenberry -- Col. 5 lines 62-67 – Col. 6 lines 1-10, Col. 6 lines 52-67**

– Col. 7 lines 1-9 and lines 24-33 – User profile, i.e. passport, stores various pieces of field

data, including name, address, etc., with each field having security levels assigned to it

which regulate who can and can not view the information];

setting the permissions relative to a given service provider so as to prevent access to at

least one selected field and grant access to at least one given field in the user profile so as to

support an anonymous transaction between the given service provider and the user by

withholding an identity of the user **[Fortenberry -- Col. 6 lines 37-46 and Col. 6 lines 52-67 –**

Col. 7 lines 1-23 and Col. 8 lines 23-67 – Col. 9 lines 1-10 – Vendors receive keys which

relate to the various security levels assigned to the fields in the profile. Therefore,

dependent upon the key provided, the vendors only have access to certain fields while other

fields are blocked. In addition, transactions between vendors can take place by using the

virtual information, rather than a person's real name, i.e. identity].

With respect to claims 21-22 and 24-25, Fortenberry further teaches wherein the user

profile contains a name field holding a name (claim 21) **[Fortenberry -- Col. 6 lines 52-54 –**

Field contains user's real name], an address field holding an address of the user (claim 22)

[Fortenberry -- Col. 6 lines 52-54 – Field contains user's address], a payment field holding

payment mechanism (claim 24) and a credit card field for holding a credit card number (claim

25) **[Fortenberry -- Col. 6 lines 52-55 – Field contains user's credit card information which**

in turn is a payment mechanism].

With respect to claim 23, Fortenberry further teaches wherein the permissions are set to block access to multiple ones of the fields by the given service provider **[Fortenberry -- Col. 6 lines 37-46 and Col. 7 lines 24-33 and lines 52-60 – Based upon key provided to given service provider, i.e. vendor, access is only allowed for certain fields and all other fields are blocked. For example, if access provider is provided the first key, the vendor is blocked access to both secret and top secret information]**.

Claim Rejections - 35 USC § 103

6.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7.   Claims 4-5 and 7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fortenberry et al. (U.S. 6,005,939), as applied to claim 3 above, in view of Kramer et al. (U.S. 5,414,852).

Regarding claim 4-5 and 7, Fortenberry teaches the invention substantially as claimed, as aforementioned in claim 3 above, but fails to explicitly teach wherein a party is granted read access (claim 4), write access (claim 5) and delete access (claim 7).

Kramer, however, discloses a system which invokes permissions for accessing data objects, the

permissions including read access, write (modify) access and delete access **[Kramer -- Col. 3**

lines 47-49 and Col. 3 lines 60-67 – Col. 4 lines 1-10].

Both Kramer and Fortenberry are concerned with protecting the accessibility of data objects.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention

was made to incorporate the providing of read, write (modify) and delete access privileges for

data objects, as taught by Kramer into the invention of Fortenberry, in order to improve data

security by limiting access to data and the actions that can be performed on it.

8.   Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Fortenberry et al.

(U.S. 6,005,939), as applied to claim 3 above, in view of Siefert (US 2002/0194179).

        Regarding claim 6, Fortenberry-Kramer teach the invention substantially as claimed, as

aforementioned in claim 3 above, but fails to explicitly teach an availability access which allows

for searching of profiles.

Siefert, however, discloses a resource management system which provides functionality to a user

which allows them to search for available user profiles **[Siefert -- Page 3 paragraph [0074]]**.

It would have been obvious to one of ordinary skill in the art at the time the invention was made

to incorporate the permission to search user profiles, as taught by Siefert into the invention of

Fortenberry-Kramer, in order to an obvious enhancement of functionality and usability for a user

who wishes to access profile information

9.   Claims 9-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fortenberry

et al. (U.S. 6,005,939), as applied to claim 1 above, in view of Hayes Jr. et al. (US

2001/0011341).

Regarding claim 9, Fortenberry teaches the invention substantially as claimed, as

aforementioned in claim 1 above, but fails to explicitly teach wherein a set of permissions

contains a list of parties that may access either the profile or field data.

Hayes Jr., however, discloses a system which stores applications for downloading to a user

system along with an access permission list defining what users, as part of a group or subgroup,

can access certain applications, i.e. applets **[Hayes Jr. -- Page 5 paragraph [0043], page 10**

paragraph [0086] and page 11 paragraph [0088]].

It would have been obvious to one of ordinary skill in the art at the time the invention was made

to incorporate the listing of groups or subgroups, i.e. users, which have access to a given

application or function, as taught by Hayes Jr. into the invention of Fortenberry, in order to

provide a definitive and explicit list of who has access to given applications or data.

Regarding claim 10, Fortenberry-Hayes Jr. teaches the invention substantially as claimed,

wherein defined groups of parties are provided for on the permission groups **[Hayes Jr. -- Page**

10 paragraph [0086] and page 11 paragraph [0088] – Groups can be created consisting of

users, upon which the permissions assigned to that group are inherited by the users

belonging to the group].

10.   Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over Fortenberry et al.

(U.S. 6,005,939), as applied to claim 12 above, in view of Ramamurthy et al. (US

2002/0091745).

Regarding claim 14, Fortenberry teaches the invention substantially as claimed, as

aforementioned in claim 12 above, but fails to explicitly teach wherein the subdivisions are

organized hierarchically and wherein the subdivisions contains additional subdivisions.

Ramamurthy, however, discloses a directory tree structure, i.e. hierarchy, which stores the

various breakdown of groups which have access to a given application or data. Each subdivision

is divided into multi subdivisions, with employees having their profiles connected in the tree

[Ramamurthy -- Pages 6 & 7, paragraphs [0105-0107]].

It would have been obvious to one of ordinary skill in the art at the time the invention was made

to incorporate the organization of subdivisions in a tree hierarchy structure with multiple

subdivisions off of one subdivision, as taught by Ramamurthy into the invention of Fortenberry,

in order to provide a robust data structure for organizing profile information that can easily and

quickly be defined and customized as organizational structures change.

11.   Claim 15 is rejected under 35 U.S.C. 103(a) as being unpatentable over Fortenberry et al.

(U.S. 6,005,939), as applied to claim 1 above, in view of Regnier et al. (U.S. 6,134,549).

        Regarding claim 15, Fortenberry teaches the invention substantially as claimed, as

aforementioned in claim 1 above but fails to explicitly teach defining groups which have a

permission access set, said access set resulting from a set algebraic operation performed on at

least two groups.

Regnier, however, discloses a system which provides secure access to a database by using client

profile permissions along with an algebraic manipulation on defined groups to provide various

customized permissions [Regnier -- Col. 6 lines 49-55 and Col. 7 lines 40-63].

It would have been obvious to one of ordinary skill in the art at the time the invention was made

to incorporate the use of algebraic manipulation on groups to provide various customized

permission access levels to defined groups, as taught by Regnier into the invention of

Fortenberry, in order to provide rapid customization of access permissions along with a variety

of group manipulations

12.   Claims 12 and 16-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Fortenberry et al. (U.S. 6,005,939).

        Regarding claim 12, Fortenberry teaches the invention substantially as claimed, as

aforementioned in claim 1 above, but fails to explicitly teach that one of the permissions is set to

a default setting.

It is well known and common in the art that when setting up any type of profile or record, default

fields for common or standard responses are filled in automatically by the system which provide

the user with the ability to modify the fields if necessary. Fortenberry discloses having the user

set up a security level field by specifying either a 0, meaning the data is clear or a 1 to indicate

the data is secure **[Fortenberry -- Col. 7 lines 24-33]**. It would have been obvious to one of

ordinary skill in the art at the time the invention was made to provide a default setting for certain

data which is typically secure, i.e. credit card information, and typically not secure, i.e. name or

address, in order to make the inputting of information easier for the user so that each field does

not need to be explicitly specified all of the time.

Regarding claim 16, Fortenberry teaches the invention substantially as claimed, a

method, comprising the steps of:

providing user profiles that hold information regarding users and are accessible via a

network **[Fortenberry -- Col. 1 lines 51-55 and Col. 5 lines 62-67 – Col. 6 lines 1-7 – Users**

store certain personal and demographic information in a database as a profile, i.e.

passport, which is accessed via the Internet];

specifying a service provider for providing services to the users **[Fortenberry -- Col. 6**

lines 37-46 and Col. 8 lines 31-32 – User provides keys to vendors, i.e. service providers,

which allow them access to the profile information]; and

granting access permission for authorized information in a selected user profile to a

selected service provider who may access the authorized information **[Fortenberry -- Col. 6**

lines 37-46 and Col. 8 lines 31-32 – User provides keys to vendors, i.e. service providers, which give them permission to access the authorized profile information of the user].

While Fortenberry does not explicitly teach a group of service providers, he does teach that the key is given to a vendor, which is then allowed access to the information. Thus, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the vendor to include more than one vendor or groups of vendors in order to be able to receive more services over the Internet. *In re Harza*, 274 F.2d 669, 124 USPQ 378 (CCPA 1960) states that "mere duplication of parts has no patentable significance unless a new and unexpected result is produced."

Regarding claim 17, Fortenberry teaches the invention substantially as claimed, as aforementioned in claim 16 above, including wherein the service providers in the selected group all provide a common category of service **[Fortenberry -- Col. 8 lines 59-67 – Col. 9 lines 1-4 and lines 28-47 – Once sub-group of providers, i.e. on-line financial databases such as VeriSign, access the information to authenticate the data for the transaction to complete].**

Regarding claim 18, Fortenberry teaches the invention substantially as claimed, as aforementioned in claim 16 above, including wherein one group contains other sub-groups, said other sub-groups containing logically related service providers **[Fortenberry -- Col. 1 lines 13-22 and Col. 8 lines 59-67- Col. 9 lines 1-4 and lines 28-47 – Vendor, i.e. merchant upon which a good can be purchased, contains a sub-group of on-line financial databases, i.e.**

VeriSign, which service as to provide a logically related service, namely, verifying the payment information submitted to a vendor by a user].

Regarding claim 19, Fortenberry teaches the invention substantially as claimed, as aforementioned in claim 16 above, including wherein the user profiles are accessible via a centralized repository and wherein the authorized information in the user profile may be accessed by service providers that did not directly solicit the accessible information from the user **[Fortenberry -- Col. 5 lines 62-67 – Col. 6 lines 1-7 and Col. 8 lines 34-40 – User profiles, i.e. passports, are stored in a central database. Vendor, i.e. service provider, accesses and obtains the information by using the passport agent, thereby, bypassing the user].**

13.   Claim 26 is rejected under 35 U.S.C. 103(a) as being unpatentable over Fortenberry et al. (U.S. 6,005,939) in view of Hayes Jr. et al. (US 2001/0011341) and further in view of Brown et al. (U.S. 6,658,415).

Regarding claim 26, Fortenberry teaches a method, comprising the steps of:

providing a user profile holding information regarding a user in fields **[Fortenberry -- Col. 1 lines 51-55, Col. 5 lines 62-67 – Col. 6 lines 1-7 and Col. 6 lines 52-62 – Users store certain personal and demographic information in a database as a profile, i.e. passport, which are organized in fields];**

providing a protocol [**Fortenberry -- Col. 9 lines 5-10 -- Protocol which enables passing of information**] that enables the getting and setting of the following:

fields in the user profile [**Fortenberry -- Col. 6 lines 52-62 -- User profile contains fields, i.e. name field, address field, for storing user information**];

access permissions for the fields in the profile [**Fortenberry -- Col. 6 lines 1-2 and Col. 7 lines 24-33 -- Each piece of information, i.e. field, contains a security permission level that restricts access to the information**]; and

permissions access permissions that specify permissions for the access permissions [**Fortenberry -- Col. 6 lines 37-46 and Col. 7 lines 51-60 -- Access permissions, i.e. confidential, secret and top secret are specified by other access permissions, namely, defining the security level on each field of information**].

Fortenberry fails to teach groups which provide members access permissions to selected field data, group access permissions that specify access information regarding groups and a schema definition for the profile.

Hayes Jr., however, discloses having groups with members which only have access permissions to certain data or programs defined by the particular group which they belong [**Hayes Jr. -- Page 5 paragraph [0043], page 10 paragraph [0086] and page 11 paragraph [0088] -- Groups are created with given access permissions upon which each member of the group inheriting those access permissions**].

Furthermore, Brown teaches a system for restricting access to content based upon a user profile stored which employs the use of a schema definition to transmit data in a common format and to provide validation [**Brown -- Col. 2 lines 20-24, Col. 5 lines 11-24 and Col. 10 lines 20-33**].

It would have been obvious to one of ordinary skill in the art at the time the invention was made

to incorporate organizing the members into groups which only have access to certain data or

programs based upon the group they belong, as taught by Hayes Jr., along with providing a

schema definition for user profiles, as taught by Brown, into the invention of Fortenberry, in

order to provide a manageable and more easily customized access list which provides a definitive

and explicit list of who has access to given applications or data and to also provide profile data

which is universally accessible to all people and all devices via the schema definition.

Conclusion

14.   The prior art made of record and not relied upon is considered pertinent to applicant's

disclosure.

- Hunt et al. (U.S. 6,496,855) discloses a system for providing a central repository of

   all personal information that an individual Internet user is prepared to give out to sites

   in order to register with a site.

- Mandato et al. (US 2001/0025280) discloses a mobile system which manages user

   profile information.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thomas J. Mauro Jr. whose telephone number is 703-605-1234. The examiner can normally be reached on M-F 8:00a.m. - 4:30p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, David A. Wiley can be reached on 703-308-5221. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

TJM
June 16, 2004

DAVID WILEY
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100